Disclosing Data

Many of us have access to Privacy Act records as part of our job at the National Institutes of Health (NIH), and we may receive inquiries or requests for personal information. In fact, the Privacy Act is personal. It's about records the government is maintaining on you and me!

Our Privacy Act requestors consist of current and former employees, patients, study participants, grantees and contractors, visitors to our campus facilities, the general public, etc. In other words, they are people who have had a relationship with us.

Paragraph 1 of Section B of the Privacy Act of 1974, as amended, provides a simple condition for disclosure:

"No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…"

However, you should know that information may be released to:

- Congressional Oversight Committee upon request by the Chairperson;
- Court Appointed Judges pursuant to a court order signed by the Judge;
- Individuals authorized by the subject of the record; and
- Parents and legal guardians of minor children.

It's also important to remember that the system manager must have a written request and be able to reasonably satisfy himself or herself of the requestor's identity before releasing any records under the Privacy Act, as amended!

Routine Uses for Disclosure

According to The Privacy Act of 1974, as amended, there are provisions of disclosure for which the written consent of an individual is **NOT** required:

- Employees of the agency with a legitimate "need-to-know" the information (i.e., they must have a valid business need to access the information);
- When required under the Freedom of Information Act (FOIA) (for which a written request must be received);
- When a "routine use" in the Privacy Act Systems of Record Notice (SORN) permits it (for a non-mandatory disclosure);
- U.S. Census Bureau (for census surveys and reporting);
- Statistical Use (only if the data cannot be used to identify an individual);
- U.S. National Archives and Records Administration (for historical purposes);

- U.S. Civil or Criminal Law Enforcement Agencies (for law enforcement purposes);
- Compelling Circumstances (if justified in describing how the release would affect the health or safety of an individual or population);
- Either House of Congress (in their oversight capacity);
- Comptroller General (for General Accounting Office activities);
- Court of Competent Jurisdiction (if the subpoena is signed by a Judge); and,
- Consumer Reporting Agency (in accordance with Title 31, Section 3711(e)).

The Privacy Act of 1974, as amended, allows an individual a certain amount of control over the information NIH collects. The individual has a right to:

- Seek access to records retrievable by their name and/or personal identifier that is contained in a Privacy Act System of Records (except for certain situations);
- Provide written authorization for their representative to act on their behalf;
- Seek records on behalf of a minor child, if they are the legal guardian or parent acting in the best interest of the minor child;
- Amend the record to change factual information; and,
- Appeal the denial of a request for an amendment.

Requesting Records under the Privacy Act

Individuals who wish to request records about themselves must:

- Submit a request in writing to the system manager listed on the Privacy Act Systems of Record Notice that covers the information collection;
- Verify their identity by providing at least one piece of tangible identification such as a driver's license, passport, alien or voter registration card;
- Specify which systems of records they wish to have searched and the records to which they wish to have access, and whether they want copies made of all or any such records; and,
- Provide the system manager with sufficient information to enable the agency to distinguish between records on subject individuals with the same name.

If an individual does not have identification papers to verify his identity, he must submit a notarized request in writing to verify his identity or certify in his request that he is the individual who he claims to be. He must also state that he understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act, subject to a $5,000 fine.

Amending Records

The Privacy Act allows individuals to seek amendment of erroneous information that is based on fact, and not opinion. The burden of proof is on the requestor seeking to amend a record.

To amend a record, the individual must:

- Submit a request in writing, except for routine administrative matters such as the change of an address or phone number;
- Include a description of the information to be amended; the reason for the amendment; type of amendment action sought, including all available evidence that supports the request.

Upon receipt of a request to amend a record, the system manager must:

- Acknowledge receipt of the written request within 10 working days;
- Make a ruling within 30 working days;
- Notify the requestor of the decision to amend the record, the time-frame in which to appeal the decision and the appellate authority. If the request is denied, the requestor must be notified of the denial, the reasons for the denial, his right to appeal the decision, and that he may submit a statement of disagreement to be associated with the disputed record and disclosed whenever the record is disclosed.

The Privacy Act recognizes that there are some instances when an individual's request for their own records may be denied. For example, disclosure may be denied, if:

- The information was compiled in anticipation of, or is being used in a civil action or proceeding;
- The information lives within a Systems of Record (SOR) that is exempt from the Privacy Act; and
- The System Notice published in the Federal Register includes certain security classifications or specific exemptions that prohibit disclosure.

Privacy Act Appeals

Individuals wishing to appeal a denial of notification, access, or amendment should:

- Submit a written request within the specified appeal time-frame to the agency appellate authority;
- Include a copy of the denial letter; and
- Include a statement of reasons for review of the appeal and requested action.

When you consider the Privacy Act from an individual's point of view, it's easy to see why these limits are placed on the disclosure of data.

If, for example, you were one of the 26.5 million veterans whose personal identity information was threatened in May of 2006, when a Veterans Affairs employee's laptop was stolen from his home, you probably felt concern or anxiety over the incident. Fortunately, the information was recovered and the Federal Bureau of Investigation (FBI)

determined with high confidence that the sensitive files were not accessed or compromised.

There are criminal penalties specified in the Privacy Act, for:

- Willfully disclosing information;
- Willfully maintaining an illegal system of records prior to the publication of a System Notice in the Federal Register;
- Sharing data with unauthorized individuals; and,
- Obtaining or disclosing data under false pretenses or facilitating others acting under false pretenses.

Criminal Penalties include:

- Misdemeanor Charge (jail time up to one year); and
- Fines up to $5,000.

There are also civil penalties specified in the Privacy Act, for:

- Refusing to amend an individual's record in accordance with his request;
- Refusing to grant access at the legitimate request of an individual;
- Failing to maintain a record that is accurate, timely, and complete to assure fairness of any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made that is adverse to the individual; or,
- Failing to comply with any other provision or rule in such a way as to have an adverse effect on the individual.

Civil Penalties include:

- Actual Damages;
- Reasonable Attorney Fees; and
- Disciplinary Personnel Actions, including removal from employment.

It is always good to keep in mind "the golden rule" of privacy –

"Treat information the way you would want YOUR information treated by others!"